

Diskreter Logarithmus

Josef Schmeißer und Fabian Grotz

25.05.2016

1 Algorithmen zur Bestimmung des diskreten Logarithmus

- Babystep-Giantstep-Algorithmus

2 Anwendungen in der Kryptographie

- Elgamal-Verschlüsselungsverfahren

Babystep-Giantstep-Algorithmus

Theorie

- Gegeben Zyklische Gruppe \mathbb{G} mit Ordnung n , Generator g und ein Element der Gruppe α
- Gesucht ist x sodass $g^x = \alpha$
- setzen $x = i \cdot m + j$
- m sollte in $\lceil \sqrt{n} \rceil$ sein
- ausserdem $0 \leq i < m$ und $0 \leq j < m$

Theorie

$$g^{im+j} = \alpha \Leftrightarrow g^j = a(g^{-m})^i$$

Theorie

$$g^{im+j} = \alpha \Leftrightarrow g^j = a(g^{-m})^i$$

Babystep

Berechne für alle j den Ausdruck g^j . Paare (j, g^j) werden in Tabelle gespeichert

Theorie

$$g^{im+j} = \alpha \Leftrightarrow g^j = a(g^{-m})^i$$

Babystep

Berechne für alle j den Ausdruck g^j . Paare (j, g^j) werden in Tabelle gespeichert

Giantstep

Berechne $(g^{-m})^i$ und vergleiche mit Tabelle. Wenn Treffer, gib $x = im + j$ aus.

Algorithmus in Pseudocode

Eingabe

zyklische Gruppe G der Ordnung n mit einem Generator g und ein Element der Gruppe α

Berechnung

- 1 Setze $m := \lceil \sqrt{n} \rceil$
- 2 Für alle $j \in \{0, \dots, m-1\}$:
 - 1 Berechne g^j und speichere das Tupel (j, g^j) in einer Tabelle
- 3 Setze $t := \alpha$
- 4 Für alle $i \in \{0, \dots, m-1\}$:
 - 1 Suche in der Tabelle nach einem Paar mit $t = g^j$
 - 2 Wenn Paar existiert gib $im + j = \log_g(\alpha)$ aus
 - 3 Wenn nicht: Setze $t := t * g^{-m}$ und fahre fort

Beispiel

- Wir nehmen eine Gruppe G der Ordnung $n = 29$ mit Erzeuger $g = 11$
- Wir wollen den diskreten Logarithmus von $a = 3$ zur Basis g berechnen, also die Lösung von $3 = 11^x \bmod 29$
- Rechnung siehe Tafel

Beispiel

- Wir nehmen eine Gruppe G der Ordnung $n = 29$ mit Erzeuger $g = 11$
- Wir wollen den diskreten Logarithmus von $a = 3$ zur Basis g berechnen, also die Lösung von $3 = 11^x \bmod 29$
- Rechnung siehe Tafel
- Lösung: $\log_{11} 3 = 2 \cdot 6 + 5 = 17$

Laufzeit

Laufzeit

hängt von Liste ab, die m -Einträge nach Babystep Berechnungen hat und durchsucht werden muss.

Mit Hashfunktionen kann laufzeit gemindert werden.

Dadurch gesamte Laufzeit bei $O(m)$ bzw. $O(\sqrt{n})$

Speicherverbrauch

Speicherverbrauch

hängt von Liste ab, die m -Einträge nach Babystep Berechnungen hat. Dadurch gesamter Speicherbedarf bei $O(m)$ bzw. $O(\sqrt{n})$

Elgamal-Verschlüsselungsverfahren

Elgamal-Verschlüsselungsverfahren

- entwickelt 1985 von Taher Elgamal
- ist ein Public-Key Verschlüsselungsverfahren
- beruht auf Operationen in einer zyklischen Gruppe endlicher Ordnung

Vorbereitungen

Der Empfänger

- 1 wählt eine endliche, zyklische Gruppe G der Ordnung n mit Erzeuger p
- 2 wählt eine zufällige Zahl $a \in \{1, \dots, n-1\}$ mit $\text{ggT}(a, n) = 1$ als privater Schlüssel des Empfängers
- 3 berechnet das Gruppenelement $A = p^a \in G$ als öffentlicher Schlüssel
- 4 veröffentlicht (G, p) und A

Verschlüsseln

Der Sender

- 1 möchte Nachricht $m \in G$ versenden
- 2 wählt $r \in \{1, \dots, n-1\}$ mit $\text{ggT}(r, n) = 1$
- 3 berechnet $R = p^r \in G$
- 4 berechnet $c = A^r \cdot m \in G$
- 5 sendet (R, c) an den Empfänger

Entschlüsseln

Der Empfänger

- berechnet $m = R^{-a} \cdot c \in G$

Entschlüsseln

Der Empfänger

- berechnet $m = R^{-a} \cdot c \in G$

Es gilt: $R^{-a} \cdot c = p^{-ra} \cdot A^r \cdot m = p^{-ra} \cdot p^{ar} \cdot m = m$

Beispiel

Wie nehmen ein Beispiel:

$p = 47$, $g = 5$ werden veröffentlicht

B wählt $b = 29$

A wählt $a = 7$

Nachricht $m = 42$

Decisional Diffie-Hellman-Problem (DDH)

Grundgedanke

Angreifer kann zwischen $\langle g^a, g^b, g^{ab} \rangle$ und $\langle g^a, g^b, g^c \rangle$ nicht unterscheiden, wenn a, b und c zufällig gewählt in $[1, |G|]$.